IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.DOI

FogChain: A Fog computing architecture integrating Blockchain and Internet of Things for Personal Health Records

ANDRÉ HENRIQUE MAYER[1], VINICIUS FACCO RODRIGUES[1], CRISTIANO ANDRÉ DA COSTA[1], (SENIOR, IEEE), RODRIGO DA ROSA RIGHI[1], (SENIOR, IEEE), ALEX ROEHRS[1], AND RODOLFO STOFFEL ANTUNES[1], (MEMBER, IEEE).

[1]Software Innovation Laboratory (SOFTWARELAB), Applied Computing Graduate Program, Universidade do Vale do Rio dos Sinos (UNISINOS), Av. Unisinos, 950, 93022-750 São Leopoldo, RS, Brazil

Corresponding author: Cristiano André da Costa (e-mail: cac@unisinos.br).

ABSTRACT The Internet of Things (IoT) adoption grows significantly and is successful in many different domains. Nevertheless, the ever-growing demand for more connected devices pushes the requirement for scalable IoT architectures capable of maintaining the security and privacy of collected data. The latter is a particularly critical aspect when considering sensitive data, e.g., medical records. One solution to address this challenge is to modify the centralized back-end model to one based on a Blockchain, changing the way IoT data is stored and shared by providing a decentralized peer-to-peer network. This technology enables naming and tracking for connected devices, and in the case of this article, features a high availability of Personal Health Records, yet protecting patients' privacy through the use of cryptography. Furthermore, the addition of Fog computing mechanisms helps to achieve real-time data processing, supports precision medicine, and avoids single points of failure. As a result, devices have a local and more resilient ecosystem for operation. In this context, this work proposes an architecture model named FogChain, which combines the technologies Blockchain, Fog computing, and the IoT for the healthcare domain. Our main contribution is the FogChain model itself, and its concept of overcoming IoT constraints by employing a differential approach, adding an intermediary Fog layer near to the edge to improve their capabilities and resources. Experiments demonstrate that FogChain can achieve a 62.6% faster response time when compared to Cloud-like Blockchain infrastructures. The results obtained from the evaluation endorses the capacity of our model in achieving its goals while retaining application performance.

INDEX TERMS Personal Health Record, Blockchain, Fog computing, Internet of Things, Distributed systems, Health Informatics

I. INTRODUCTION

Internet of Things (IoT) refers to the network of physical objects embedded with software and sensor devices capable of communicating over the Internet for information exchanging [1]. Such devices collect, process, and exchange vast amounts of data from the surrounding environment as well as privacy-sensitive information without any human intervention [5]. When applied to the healthcare context, such devices compose the Internet of Health Things (IoHT) [12], which consists of a network of interconnected objects exchanging and processing medical data focused on improving medical processes. Such environments impose additional restrictions to technologies that handle such data due to its sensitivity and confidentiality issues. As a result, the sensitive nature of such networks makes them appealing targets for cyberattacks [15]. The privacy of collected data may be at risk when stored and managed by outsourced companies on centralized servers (e.g., cloud hosting). In such cases, the main concerns regard data leak caused by cyberattacks the cloud providers migh suffer [10].

In the last few years, the rise of Blockchain technologies offer secure solutions providing trust, accountability, traceability, and integrity of data sharing, to secure distributed data across organizations [18], [24], [40]. That enables solutions to try Blockchain capabilities in the context of healthcare to overcome the privacy and security problems. Currently, Blockchain is the most popular form of distributed ledger technology (DLT). Its features enable IoT applications that

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3109822, IEEE Access

require a trusted third-party to be decentralized [23]. Thus, the need of a central authority is removed without compromising the functionalities and guarantees of applications [9], [40]. The use of cryptography, a key characteristic of Blockchain networks, brings authoritativeness behind all the interactions in the network [9], where Blockchain has a fundamental role in registering and authenticating all operations performed on IoT devices data [10]. This technology could reinvent the way patient's electronic and personal health records (EHR and PHR) are shared and stored by providing safer mechanisms for health information exchange (HIE), by securing it over a decentralized peer-to-peer network, thus making the health records more available, efficient and secure [31], [37].

Regardless of the security challenges, IoHT environments require extra performance when it comes to time response. Having quick access to processed information from patients allow fast decision-making by the medical team. That is crucial to improve medical services and deliver a high quality of service for patients. Frequently, current IoT and healthcare solutions rely on Cloud computing resources to provide processing of data from sensors [3]. However, such solutions impose data to be transferred to cloud servers, which can be physically distant and increase network latency. That impacts the agility of the system to process and produce feedback from data to the medical team. Moreover, recent study predicts that centralized clouds, frequently used in current IoT systems, will be unlikely to deliver satisfactory services to customers [46]. From the core to the edge of the network, adoption of Fog computing alternatives are encouraged and represent a layered service structure that is an extension of the cloud computing paradigm [46].

Fog computing is able to provide faster cloud-like services such as storage, computing, and networking capabilities closer to users and devices, by extending the data management field of the cloud and increases the accessibility of IoT resources [49]. These abilities are a consequence of allocating Fog nodes closer to the IoT devices, at the edge of the network, thus reducing communication's latency and promoting closer to real-time communication with the Things layer [6], [36], [46]. Given that IoT devices spend most of their available energy and computational resources to execute core application functionalities and data collection, supporting extra security and privacy turns to be quite challenging [15].

Currently, to the best of our knowledge, there are no studies that focus on integrating Fog and Blockchain technologies to the IoHT domain. In this context, this article proposes FogChain, a model for integrating Fog and Blockchain for PHR management. FogChain allows close to real-time data processing given that the patient's health records are to be locally available in a Fog computing layer, thus improving physicians response time and decision making [42]. We developed a prototype of the model using JavaScript and employed Hyperledger Fabric distribution in the Blockchain level of the model. Experiments demonstrated improvements up to 40.3% in response time when comparing FogChain with a Cloud solution. In summary, the main goals of the current research are as follows:

- Build a model for integrating Blockchain and Fog Computing to manage PHR in the IoHT field;
- Improve response time on registering PHR information in the Blockchain and, consequently, make health data available quickly.

We have organized the article as follows. Section II introduces background concepts related to this research. Section III presents related research carried for other authors in the same domain this research focuses on. Following, Section IV describes the FogChain model, including design decisions and its architecture. Then, Sections V and VI present the evaluation methodology and results, respectively. Finally, Section VII concludes the article with final remarks and future directions.

II. BACKGROUND

This section gives a brief overview of the main technologies employed in this study: Blockchain, IoHT, and Fog Computing. The concept of IoT may have different interpretations depending on the context where it is applied. For instance, the things-centric (e.g., from the sensor's point of view) could potentially be patient-centric by consisting of interconnected objects with the capacity of exchanging and processing data to improve patient's health [12]. In this sense, IoHT consists of interconnected objects with the capacity of exchanging and processing data to improve patient health [12]. It relies on the use of wearable sensors and other medical devices that communicate via RFID, NFC, or Bluetooth with computing nodes to extract information from the medical environment. They collect and transmit data to remote servers for further processing to generate feedback aiming at improving medical processes. The main goal in such environments is to monitor sensor data providing information regarding the patients, medical staff, equipment, and even the environment.

In turn, Blockchain is gaining attention in the last few years in many different fields. It consists of a Peer-to-Peer (P2P) DLT for transactions that do not require a central authority, eliminating the need for third-party verification [10]. A Blockchain contains sets of chained blocks of transactions and every block contains a hash of the previous block. In summary, a Blockchain is a distributed ledger protocol originally associated with Bitcoin [16]. It uses public-key cryptography to create an append-only, immutable and time-stamped chain of content [37]. It was originally designed for keeping a financial ledger, but the Blockchain paradigm can be extended to provide a generalized framework for implementing decentralized compute resources even into the Healthcare ecosystem [16]. Blockchain technologies are a promising means to address the barriers with distributed health records by forming a unified view of the patient's personal health records. The process of collecting vital signs in hospital wards varies, and different approaches are used worldwide. In some cases, data is only manually collected

and stored in spreadsheets that are discarded after the patient is discharged [12], and is precisely at this point where Blockchain technology may contribute and become a viable solution for health records management.

Finally, Fog Computing may be viewed as a layered service structure that is an extension of the Cloud Computing paradigm. It is composed by low-energy computing nodes with limited hardware specifications. They are able to provide faster Cloud services such as storage, computing, and networking capabilities to end users, with Fog nodes located near the devices at the edge of the network [46]. The Fog Computing infrastructure may support distributed applications with the addition of a new intermediary layer between the devices and back-end services, potentially facilitating their integration [39]. It may help preventing unavailabilities originated by delays and latency gaps over the public Internet, which are of the most concerns on healthcare information exchange applications [48]. In summary, the Fog Computing plays an important role in the healthcare domain, and has potential to be a natural technology integrator. Recent studies point out benefits of adopting it on organization's internal infrastructure, and these benefits could be extended to patients in clinics and hospitals.

III. RELATED WORK

This section presents literature studies related to our scope of research. We followed the principles of the systematic literature review [25] to reach to the most relevant articles in the scope of Fog Computing, Blockchain, and IoHT. First, we defined the following set of keywords to compose a search query to be applied to several article databases:

```
"blockchain" AND ("intertet of things"
  OR "iot") AND ("fog computing" OR
"fog") AND ("healthcare" OR "health")
  AND ("health record" OR "medical
 record" OR "EHR" OR "PHR" OR "EMR")
```

Using the string above, we queried six different scientific databases: (*i*) IEEEXplore[1], (*ii*) PubMed Central[2], (*ii*) Google Scholar[3], (*iv*) Springer Link[4], (*v*) ACM Digital Library[5], and (*vi*) Science Direct[6]. We chose these databases to cover a broad set of scientific literature published in different areas. In each database, we built the search query filtering articles from the last ten years to reach the most recent studies in the area. Following, Section III-A details each selected article from our methodology, while Section III-B presents some discussion and open issues that drive our research.

[1]https://ieeexplore.ieee.org
[2]https://www.ncbi.nlm.nih.gov/pmc/
[3]https://scholar.google.com/
[4]https://link.springer.com/
[5]https://dl.acm.org/
[6]https://www.sciencedirect.com/

A. STATE-OF-THE-ART

In [4], the authors present a multi-tier framework for integrating IoT in EHR systems using Blockchain and Cloud technologies. The proposed system uses Elliptic Curve Cryptography (ECC), which may introduce more security strength compared to other cryptography approaches. However, the solution does not provide the health records locally. Instead, they are accessible through a Blockchain Cloud provider, which is not covered in the article. In [19], the authors propose the Secured and Smart Healthcare System (S2HS) to provide security and privacy in healthcare systems. The study employs a Wireless Sensor Network (WSN) architecture to collect EHR data from IoT wearable devices. Blockchain is employed to encrypt and standardize the data before storing it on the Cloud.

Moreover, [38] introduces a framework for sharing economy services in smart cities combining IoT, Blockchain, and Edge technologies. The authors propose AI solutions at the Edge of the network to process data from IoT devices across several domains. The Blockchain composes the security layer responsible for validating and encrypting transactions. The core of the system relies on decentralized Cloud platforms in which the IoT data is stored. In [47], the authors propose a healthcare data sharing model to reduce data fragmentation and allow patients better control of their data. The model consists of a dual-network architecture for mutable and immutable data. The latter employs Blockchain to provide security and privacy. The strategy requires healthcare providers to manually upload the information of data streams to the Blockchain service.

Furthermore, [48] present an Fog architecture to manage medical records using Blockchain and Cloud. The main goal of the solution is to provide patients the ability to control the access to their medical data. Fog nodes are placed near to the sensors to provide a decentralized Blockchain authorization layer and make data available close to the applications. The article describes a case study that evaluates the performance, privacy, and interoperability requirements of the proposed architecture in a home-centered healthcare scenario. In [52], the authors develop a framework for integrating IoT systems, Fog and Cloud infrastructure. The proposal consists of several Fog nodes close to sensors providing computing capabilities and data processing. The Cloud infrastructure works as a back-end which is required when Fog nodes are overloaded. In addition, Blockchain is employed in the Fog layer to ensure integrity of confidential data. The study does not focuses specifically on EHR, however the authors perform a sleep apnea analysis as case of study.

In [21], the authors propose a Blockchain-based framework focused specifically on storage and management of EHRs. The strategy employs multiple smart contracts to separate different types of information. The main goal is to provide privacy and control over the records to the patients. In turn, [2] proposes the EdgeMediChain architecture to facilitate medical data exchange by combining Blockchain and Edge infrastructure. It consists of an authentication and

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3109822, IEEE Access

authorization framework for health data sharing coming from IoT medical devices. The main contribution is the ability of the architecture perform data processing from several sensors in parallel through Edge-mining pools. Each mining pool consists of several Edge nodes that process data from sensors within a geographical location. Also focusing on data sharing, [27] seek patient information exchange among several hospitals. The authors propose a framework employing Blockchain to store historical data from patients using smart contracts.

B. DISCUSSION AND RESEARCH OPPORTUNITIES

The current state-of-the-art contains several studies that focus on bringing Blockchain to industry and healthcare sectors. From the studies gathered according to our review methodology, the most common technology that outstands is Blockchain. In the last few years, Blockchain is gaining attention due to its capabilities to provide a decentralized way of protecting data. In general, proposals make use of smart contracts to validate transactions in medical records. Through them, systems aim to give to the patients the power of controlling who can access their medical data. Besides, solutions employ Blockchain to guarantee data integrity and avoid misuse of sensitive data.

Although having Blockchain in common, studies differ on the technologies they integrate in their solutions. For instance, on the one hand, most of the studies employ Cloud infrastructures to provide medical data remotely [4], [19], [38], [48], [52]. That imposes the systems to rely on network connections that may suffer from high latency problems and, consequently, provide poor quality of service for end-users and applications. On the other hand, few studies employ Edge infrastructures to their solutions [2], [38]. In such cases, the Edge infrastructure provides data processing capabilities closer to the sensors with focus on load distribution. That allows the system scalability focusing on a wide deployment of a smart city or aggregation of several hospitals.

Looking at Table 1, only two articles include Fog infrastructures in their strategies [48], [52]. In particular, this strategies employ Fog nodes to provide closer computing capabilities to applications. However, they also require a Cloud back-end infrastructure to support overload situations due to their Fog layer be limited. Given the context, there is a lack of studies focusing specifically the integration of Fog and Blockchain for IoHT without requiring a Cloud infrastructure. The requirement of Cloud infrastructures imposes the strategies to integrate their environment with third-party providers which may not be ideal for patients. That demonstrates a research opportunity that drives the current study.

IV. FOGCHAIN MODEL

In this section, we describe the proposed model called FogChain. As the name suggests, FogChain comprehends the union of Fog computing and Blockchain technologies, which means we aim to have both co-existing, collaborating, and running in the same container at a Fog computing level. While default cloud-hosted IoT and IoHT applications struggle with significant latency issues caused by Internet network congestion and traffic [11], FogChain employs Fog computing as a middleware layer between sensor devices and the Blockchain which could better suit with the IoHT needs. Figure 1 depicts FogChain's main innovation compared to traditional solutions. FogChain introduces Fog nodes that run Blockchain peers closer to the sensors. The main idea is to decrease latency on PHR Blockchain operations and to provide a faster response for decision-making.

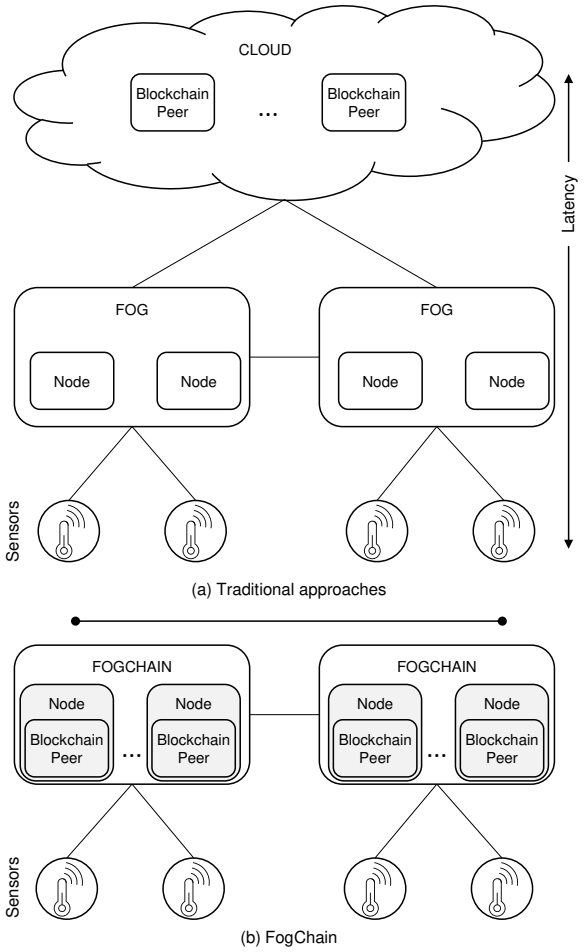

FIGURE 1. Comparison of traditional infrastructures (a) and FogChain main idea (b).

FogChain enables real-time data processing, storage and decision making by given *smart contracts* conditions satisfied. Whenever dealing with critical and or sensitive information, the response time is crucial and must be taken into account. Approximating the Blockchain peer to the IoHT devices through hosting itself a Peer inside of the Fog attempts to reduce the distance physical gap between components.

Considering possible FogChain's applications for the healthcare domain, it could be employed into healthcare organizations' infrastructures such as hospital departments or wards, handling its internal demands. Also, it could be pos-

TABLE 1. Related work comparison.

Article	Technologies	Platform	Applications	Smart-contracts
[4]	Blockchain, and Cloud	Ethereum	Healthcare	✓
[19]	WNS, Blockchain, and Cloud	DLT	Healthcare	✓
[38]	Blockchain, Edge and Cloud	Ethereum	Cross-industry	
[47]	Blockchain	DLT	Healthcare	✓
[48]	Fog, Blockchain, and Cloud	Ethereum	Healthcare	✓
[52]	Fog, Blockchain, and Cloud	DLT	Cross-industry	
[21]	Blockchain	Etherum	Healthcare	✓
[2]	Blockchain, and Edge	Etherum	Healthcare	✓
[27]	Blockchain	Etherum	Healthcare	✓
This study	Blockchain, and Fog	Hyperledger	Healthcare	✓

sible to have a FogChain inside patients' rooms, handling its sensors and environment information collected from devices.

The concept behind the model is driven by the idea of employing Fog computing architecture to improve Blockchain and IoHT integration, aiming to reduce network latency and increase resources availability near the edge. Besides, the decision to propose and build a viable solution to the health domain, possibly contributing to future research, implementations and taking the patient to the center of the solution.

A. DESIGN DECISIONS

The design of FogChain takes into consideration the following statements:

1) The model focuses on building a feasible solution for the healthcare domain, possibly contributing to future research and implementations;
2) FogChain employs Fog computing architecture to improve Blockchain and IoHT integration, aiming at reduction of network latency and increasing availability of resources near the edge;
3) Focus on PHR data to increase patient control over its medical information;
4) The model design adopts open-source projects and structures on the application's development.

We focused the conception of this model on designing a Blockchain-enabled solution for safer PHRs storage, supported by the Fog computing architecture providing performance boost for the application, improving the health things capabilities and ultimately the patient's experience. Hence, it is safe to say that we focused the scope of this project entirely on medical informatics field. However, we understand that the model, as it is today, could be used in different domains, as long as some adaptation is made in the Blockchain data structure.

B. ARCHITECTURE

The design and its components aim at supporting PHR management through the employment of Fog computing architecture, where a local Fog layer is combined with Blockchain and IoHT technologies to suit better the requirements identified in the previous steps of research and literature review. Thus, Fog computing-based techniques are employed to ensure high availability and performance, and Blockchain-based strategies were used to provide the privacy and tamper-proof required in the healthcare domain. Figure 2 depicts FogChain's architecture showing its components and iterations. Four main components compose the architecture: (*i*) IoHT Layer; (*ii*) Fog Layer; (*iii*) Blockchain Peers; and (*iv*) Smart Contracts. The next subsections detail each component and how the communication process works.

1) IoHT Layer

The first interaction with the IoHT devices is given through an internal component named IoHT++. It is responsible for exchanging messages and communicating with devices, providing some level of protocol interoperability by supporting various protocols and standards. IoHT devices are the points of contact with the physical world [9]. Devices belonging to a wireless sensor network are often limited in terms of computing capacity, storage, memory, and energy availability [35], and for this reason, usually the data is not stored in the devices themselves, but instead sent to the Fog layer. There, the middleware handles communication protocols known by the Health Things, including CoAP (Constrained Application Protocol), MQTT (Message Queuing Telemetry Transport), and HTTP (Hypertext Transfer Protocol).

2) Fog Layer

The Fog Layer is located between the IoHT devices and the Blockchain services. It comprises a solution based on Fog computing, where its technology is used for scaling solutions for Cloud computing, being able to provide storage and computation close to the end-user and edge devices [32]. Also, FogChain has mechanisms to provide further communication and interoperability capabilities for devices and being responsible for dealing with communication protocols, filtering and validating data collected and finally, transacting with Blockchain network through API.

The Fog layer of our model aims to run at the border of the Edge, consisting of a Fog computing enabled environment, where our proposed architecture dispose many of its features, as illustrated in Figure 3. It can be described as a middleware component providing microservices responsible for handling, filtering and validating incoming data from

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3109822, IEEE Access

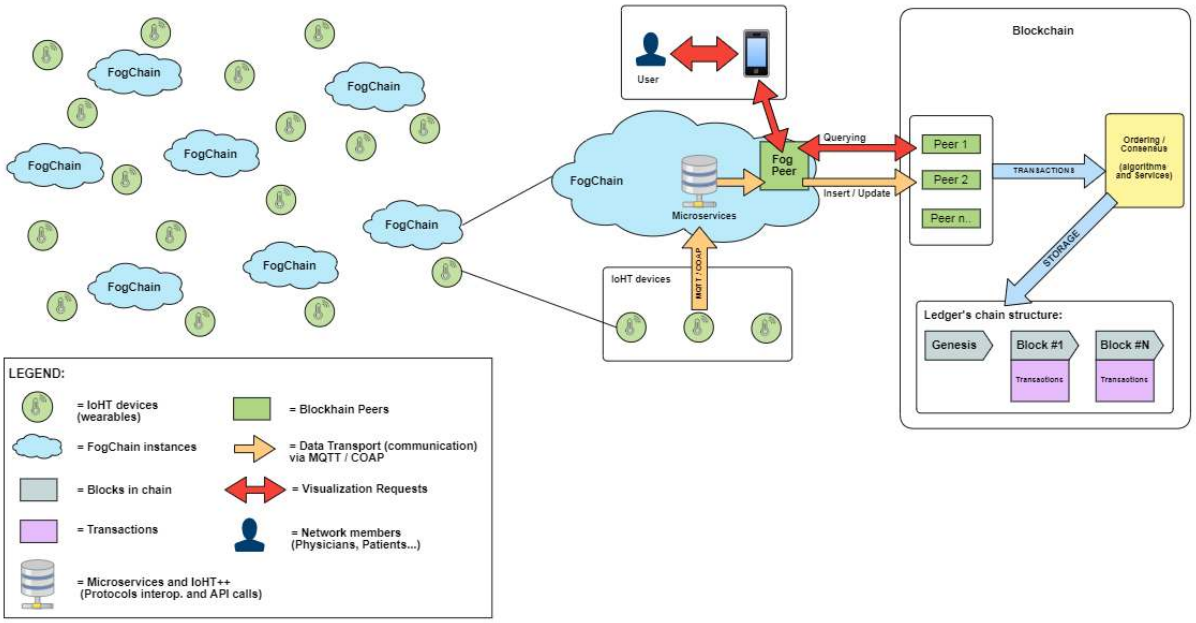

FIGURE 2. FogChain's macro visualization.

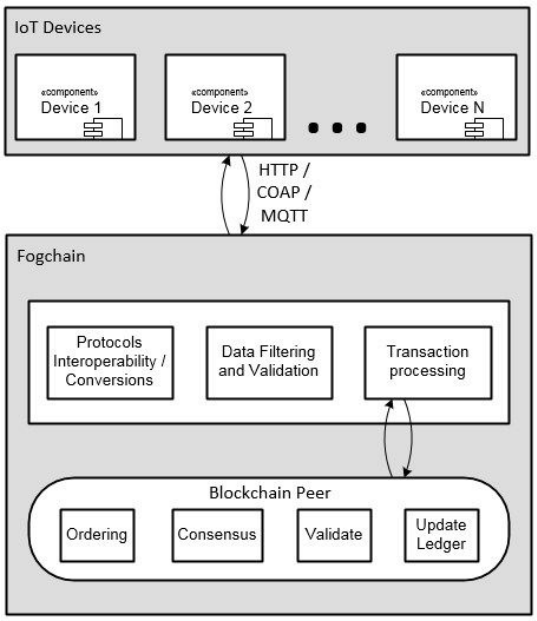

FIGURE 3. FogChain internal view structure and components.

edge devices, prior to process requests to be persisted in the Blockchain ledger.

The point of contact with the Edge devices is given through the IoHT++ microservice. Working as an entry-point, it is responsible for the communication protocols interoperability support, originated from the Nightbus (IoT++) project implementation [50] and to be available in all FogChain's instances. IoHT++ has two main internal components which are the middleware core and I/O boundaries. The first can be described as a message broker with general publish/subscribe capabilities. It divides messages into topics (categories of messages) and allows for multiple interested clients to both produce and consume messages from topics. Its implementation uses the Apache Kafka software platform, which is a distributed publish/subscribe messaging framework made available by the Apache Software Foundation [50].

Apache Kafka translates incoming client communication semantics into messages that are produced in the middleware core or consume messages from the core, communicating them to the clients. These boundaries are configured and executed in separate processes and were implemented by the original authors as services using the Clojure programming language, running on top of the Java Virtual Machine (JVM): MQTT Subscriber, MQTT Publisher, CoAP Server, CoAP Client, and HTTP Client.

Such communication protocols are supported to exchange information with IoHT devices, where its environment is usually heterogeneous, allowing devices to communicate in different protocols and channels, thus, aggregating some level of protocol interoperability necessary to our model. Whenever a new message successfully passes through the entry-point and is forwarded to the internal FogChain microservices, the incoming data is validated to prevent blank, null, or corrupted information. Moreover, a filtering function is applied, where it is possible to determine which information should be stored in the distributed ledger or to be discarded. For instance, if a wearable device is collecting multi-parametric values, this filtering function allows us to decide which parameters are essential and should be broadcasted to all peers of the Blockchain.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3109822, IEEE Access

3) Blochchain Peers

The Blockchain peers are designed to be set in place over a consortium network for a more secure health information exchange (HIE) among participants and to improve clinical data availability near the Edge. In terms of data structure, the Blockchain can be configured to support storage and organization into existing data formats and open standards already established in the health sector, such as FHIR and openEHR.

The IoHT devices' hardware usually are too restricted to actively contribute to the Blockchain network since consensus algorithms are complex and require large processing capacity and CPU storage capacity. To overcome these limitations, FogChain model proposes to add the Blockchain Peer inside the Fog instances, where ideally hardware tends to be more robust. Each FogChain peer has a copy of the ledger and may actively contribute to the network through helping to achieve consensus among existing peers.

This entire transaction workflow process helps to achieve consensus because all peers have reached agreement on the order and content of transactions, in a process that is mediated by orderers. The consensus is a multi-step process and applications are only notified of ledger updates when the process is complete. FogChain employs the Hyperledger Fabric[7] framework to implement distributed ledgers. Hyperledger Fabric allows the development of Blockchain applications, and it is currently adopted by several solutions [51]. By employing this framework, FogChain inherits the Practical Byzantine Fault Tolerance (PBFT) algorithm to reach the consensus among all nodes. Studies demonstrate that this algorithm can achieve better performance compared to others [51]. The algorithm requires at least $3f + 1$ nodes (n) to participate in the process, where f represents the number of faulty nodes, which can be achieved by $f = \frac{n-1}{3}$.

The process where participants (patients and physicians) join the network may be facilitated by the employment of smartphones interfacing with the FogChain and acting as a thin-client to the network, for instance. This thin-client is supported by the Hyperledger Fabric and represents the entity that acts on behalf of an end user. It must connect to a peer to communicate with the Blockchain. The thin-client can connect to any peer of their choice and submit transaction proposals. Figure 4 depicts a front-end design concept to interface with FogChain back-end API and services, and are better described as follow:

(a) A welcome screen for users (patients and physicians) permitting identification and authentication through their public keys and or QR code. It should allow new users to register (create wallet) and existing users to effectuate login on the platform;
(b) Patients are allowed to visualize and manage their PHR fragments;
(c) Each patient is responsible for whom they decide to share their health records, for example, by informing the physician id.

4) Smart Contracts

Smart Contracts are self-executing programs and protocols stored in Blockchain that facilitate, verify, and guarantee the execution of a contract between members of the network. For example, a patient allows/authorizes a physician to visualize their medical history. These programs provide the ability to directly track and execute complex agreements between parties without human interaction [35].

In the healthcare scenario, smart contracts may be very useful, especially in cases where it is possible to define thresholds for collected data, thus, having smart contracts executed automatically in the background, which could help in decision. For instance, in a scenario where a patient's heart rate exceeds the established limit, the smart contract could automatically trigger an event on the network notifying the physician of the existing risks.

Smart contracts may feature improvements on the interaction between patient and health providers, by automating and executing agreements predefined over the parties. For instance, evaluating healthcare information collected by IoHT devices, such as multi-parametric devices for vital signs, and comparing these readings with customized threshold values. It could trigger notification events or alerts for the patient itself or healthcare providers such as physicians and nurses when these thresholds exceed. This process provides many possibilities to extend the network and assisting interactions between patients and healthcare providers.

V. MATERIALS AND METHODS

This section describes an experimental evaluation methodology carried out to test FogChain. We highlight that this evaluation aims at developing and deploying a FogChain infrastructure in the laboratory, focusing on comparing FogChain to a traditional Cloud strategy. A multi-organization Blockchain network is in our scope, where each organization may represent a clinic or hospital for example, and each organization is allowed to have multiple Peers spread over its infrastructure, with each Peer encapsulated into a FogChain instance.To test the feasibility of the model, we managed to implement and benchmark the solution, aiming to evaluate not only application throughput, but also the impact of a Fog computing environment to mitigate latency on the interaction between edge devices and the Blockchain network.

Backed by the Blockchain as a repository for the health records we created a Fog-enabled environment serving as a middleware. The core of our FogChain architecture is written in JavaScript language, supported by the Node.js runtime to be available in all FogChain instances and all programming can be seen in our code repository[8]. It features microservices

[7]https://www.hyperledger.org/use/fabric

[8]https://bitbucket.org/uhospital/fogchain/src/multi-org/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3109822, IEEE Access

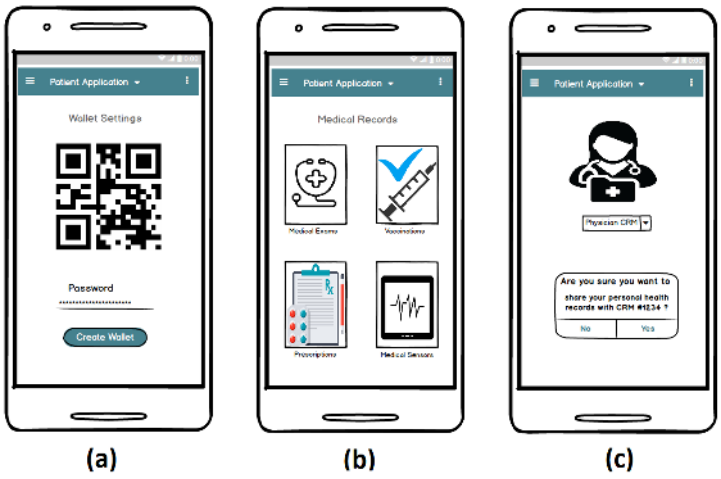

FIGURE 4. FogChain's App wireframe.

to be run locally, providing surrounding services to easy communication with Edge devices while processing requests, filtering and validating data before sending it to the local Blockchain Peer.

Regarding the Blockchain to be used in our implementation, it is possible to state that currently there are a set of available framework. To find out which Blockchain platform suits the best for our model we did a research based on our requirements and outcomes are presented in Table 2. The table compares potential available platforms, thus identifying possible strengths and weaknesses in advance for our application model. For means of implementation, we have chosen the Hyperledger Fabric Blockchain distribution, which is a DLT solution, with an open-source license made available by The Linux Foundation, and is in line with our demand given its permissioned aspect, modularity, tool support, no-fee, and project maturity.

The Hyperledger project was designed for corporate and organizational architectures, with a set of customizable rules, allowing, for example, to operate with different consensus protocols, such as PBFT, Kafka, SOLO, among others. It differs from other Blockchain platforms because it focuses on the development of private and authorized networks, mainly suitable for organizations, rather than a public and open network. It does not allow unknown identities to participate, thus, allowing the location of medical records to remain secure and restricted to hospitals and clinics infrastructure. Hyperledger's Blockchain design does guarantee transaction's integrity by submitting them through three main stages of a workflow process:

1) **Transaction Proposal**: applications generate a transaction proposal which they send to each of the required set of peers for endorsement;
2) **Ordering and packaging transactions into blocks**: it receives transactions containing endorsed transaction proposal responses from many applications, and orders the transactions into blocks;
3) **Validation and commit**: involves the distribution and subsequent validation of blocks and transactions, before it can be persisted to the ledger. Every transaction within a block must be validated in order to ensure that it is valid and has been consistently endorsed by consensus peers.

To build this network, a set of tools were employed for the development of the network and its middleware, for example, the Hyperledger Composer, which is a collaboration tool, distributed by the Linux Foundation and built with JavaScript, including Node.js, NPM, and CLI.

A. IMPLEMENTATION

Figure 5 depicts the components used to implement the Fog Layer of the architecture. One of the first requirements to create our FogChain implementation was to start defining and modeling who would be able to join the network. Specifying what kind of information and in which format data would be stored. For that, an important feature of the Hyperledger Composer was handy, the object-oriented modeling language that is used to define the domain model for a business network definition and can be used to express information or knowledge.A Hyperledger Composer model file is usually composed of a single namespace with all resource declarations, and a set of resource definition syntax for assets, transactions, participants, and events. The FogChain's Blockchain network is designed to have two main types of participants. Listing 1 presents their modeled interactions and attributes.

Listing 1. Hyperledger's Composer model file.

```
participant Patient identified by cartaoSUS {
    o String cartaoSUS
    o String name
    o String dob
}

participant Physician identified by physicianId {
    o String physicianId
```

TABLE 2. Blockchain platforms comparison.

	Ethereum	Hyperledger Fabric	Corda	MultiChain
Platform Description	Generic blockchain platform	Modular blockchain platform	Specialized distributed ledger platform for financial industry	Based on bitcoin's blockchain, for multi-asset financial transactions.
Decentralization	Yes	Partially	Partially	Partially
Transaction Model	Contract–message	Contract–message	Input–output	Input–output
Privacy Features	Public (Permissionless) - Everyone can see transactions history	Private (Permissioned) - Only members can see transactions history	Private (Permissioned) - Only members can see transactions history	Private (Permissioned) - Only members can see transactions history
Governance	Ethereum developers	The Linux Foundation	R3 Consortium	MultiChain developers and Coin Sciences Ltd
Smart Contracts	Smart contract code (e.g., Solidity lang.) with Deterministic execution	Smart contract code (e.g., Go, Java)	Smart contract code (e.g. Kotlin, Java) and legal contract (legal prose)	none
Consensus algorithm	Proof-of-Work (PoW)	Pluggable framework (generally PBFT)	Pluggable framework (multiple approaches)	Mining diversity scheme
Consensus Level	Ledger level	Transaction level	Transaction level	varies
Currency / Token	Ether (ETH).	None	None	Native multi-currency support.
Code visibility	Blockchain	Counterparties + endorsers	Counterparties + dependents	Blockchain
Transactions per second (TPS)	~15 TPS	~1.000 TPS	Varies	500-1000 TPS
Mining / Transaction Fees	Yes	No	No	No
Niche	cross-industry	cross-industry	initially financial sector	financial sector
Block Interval	~15s	N/A (Batch configuration)	N/A	customizable

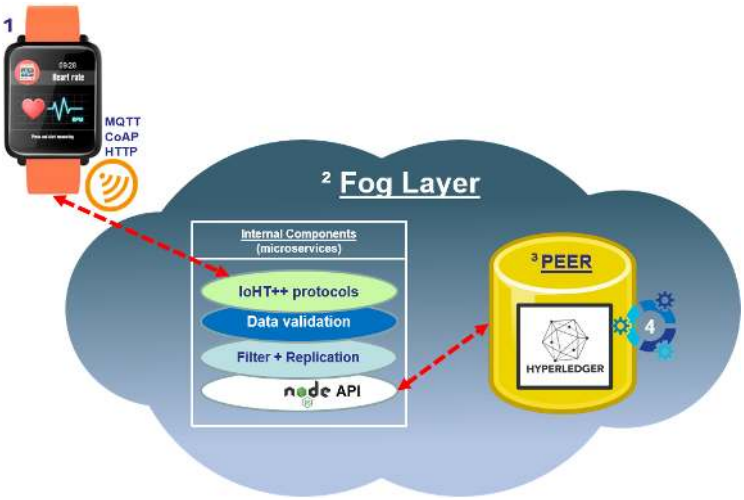

FIGURE 5. FogChain's protoype layared visualization.

```
        o String name
        > Patient[] myPatients optional
}

asset MedicalRecord identified by recordId {
        o String recordId
        o String format
        o String description
        o String offchainDataLink optional
        > Patient owner
        > Physician authorizedPhysicians
}

transaction grantAccess {
        > Physician authorisedToModify
        > MedicalRecord medicalRecord
}

transaction revokeAccess{
        > Physician revokeThisPhysician
        > MedicalRecord medicalRecord
}
```

On the one hand, the Patient entity represents any person receiving or registered to receive medical treatment. During his life he may have many medical records entries. The Patient gets to choose with who he shares his medical records, where only Physicians allowed by the Patient may see his medical history. On the other hand, the Physician entity represents any medicine practitioner working in the healthcare system. It may interact with the Patient's medical records if so the patient allows them. These two well-defined types of participants can only interact with each other through pre-defined transaction operations grantAccess and revokeAccess, where they exchange permission over the Medical Record asset. These two operations allow us to grant to the patient full control over their PHR.

While designing the Blockchain's data structure to better scale and support the vast and varies amount of healthcare

data, we came to the creation of an important feature to add flexibility regarding the size of the transaction's body, where an optional field named "offchainDataLink" may be present on the patient's Medical Record asset. The off-chain approach allows the storage of more heavyweight information such as clinical images (e.g. X-Ray), into external file system servers (off the chain) as per example the IPFS, a peer-to-peer distributed file system that seeks to connect all computing devices with the same system of files.

To establish boundaries among what participants can or can not do, share or access, the Hyperledger Composer provides an access control language (ACL) that provides declarative access control over the elements of the domain model. By defining ACL rules we can determine which users/roles are permitted to create, read, update or delete elements in a network's domain model. A code snippet presented in Listing 2 we do exemplify few of our network rules built to protect participants level of control over other participants and assets (health records).

Listing 2. Hyperledger Composer ACL rules example.

```
const NS = 'br.unisinos.uhospital.ehr';

rule LimitAccessToAuthorisedPhysician {
  participant(h): NS + ".Physician"
  operation: READ, UPDATE
  resource(m): NS + ".MedicalRecord"
  condition: (...)
  action: ALLOW
  description: "A physician may update a medical
   record to which he has permission"
}
```

Regarding the smart contracts on Hyperledger it is also referred to as chaincode in the Hyperledger Fabric documentation.

B. EVALUATION METRICS

Prototyping is a method that confronts users with a partially implemented model of a system intended to obtain quick feedback, for example, on its appearance and/or performance. It is especially useful when it is applied together with the benchmark method. The benchmark tests are used to evaluate the performance of information systems and to test their compliance with user requirements. In general, benchmarking is considered a systematic tool that allows, through metrics, to pursue and determine whether a process and or application is performing at its best. It allowed us to make improvements on the model and adapt specific components, usually with the aim of increasing some aspect of performance and is employed as a continuous process in which we continually seek for performance improvements [17].

To obtain meaningful metrics to be monitored and assessed during our experiments and analysis, we employed the Goals, Questions, and Metrics (GQM) approach (see Figure 6). GQM is a software metric approach in software engineering that proposes steps for identifying correct metrics for the creation and maintenance of a software system and clarifying which variables are essential to take into account during

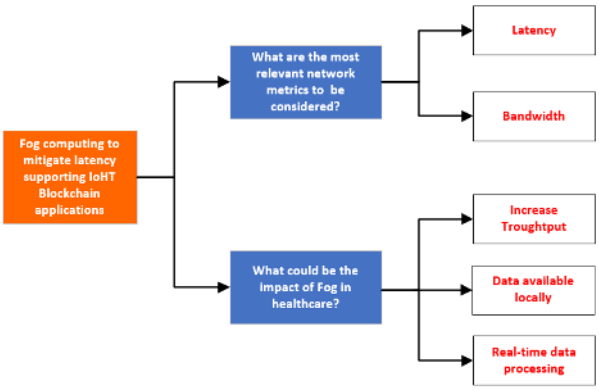

FIGURE 6. GQM - The Goal Question Metrics approach.

simulations and test executions. It is carried by identifying a set of quality and productivity goals to improve system performance. From those goals and based upon models of the object of measurement and metrics, we derived questions that define those goals as completely as possible [7]. Given the GQM approach, we selected the latency and throughput metrics as evaluation goal. Equations 1 and 2 define the $Latency$ and TPS (Transactions Per Second) metrics, respectively. In Equation 1, $t^i_{request}$ corresponds to the time a request i is sent and $t^i_{response}$ is the time the response for this request i arrives. This particular equation computes $Latency$ in milliseconds (ms). In turn, in Equation 2, TPS is achieved by dividing the total number of requests n by the total time (in seconds) taken to process all requests. We selected these metrics since they are commonly employed to evaluate the performance of Blockchain applications [51] .

$$Latency(i) = t^i_{response} - t^i_{request} \tag{1}$$

$$TPS = \frac{n}{\frac{1}{1000} \times \sum_{i=0}^{n-1} Latency(i)} \tag{2}$$

C. INFRASTRUCTURE AND CONFIGURATION

To evaluate the model and verify FogChain components' integration, we implemented and configured it on a local Fog environment, responsible for processing and storing medical data information locally. For means of testing, we collected data originated from a clinical vital signs dataset provided by "The University of Queensland" [29] institution. The local environment is composed of a physical server with Ubuntu 16.04 (64-bit) Operating System, Intel Xeon E5-2620v4 2.1GHz processor, 32GB RAM, and HDD SAS 600Gb RAID 5 (10,000 RPM). The Hyperledger Fabric Blockchain was installed and configured to run on containers in this physical machine as components of the FogChain. In particular, these containers share the physical machine resources, which makes them less powerful than the physical machine. As a consequence, these less powerful containers

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3109822, IEEE Access

mimic Fog nodes which are characterized by having less computing power than physical servers.

All libraries and dependencies were managed through Node.js and Node Package Manager (NPM), having all of our modeling and configurations in place, turning our network finally available for tests. The next step was writing an application that reads columns of the aforementioned vital signs dataset [29], such as electrocardiogram (ECG) and blood pressure, having each record becoming a transaction proposal, to be validated and persisted on the ledger.

To compare our solution with a Cloud infrastructure, we configured a similar environment. Figure 7 depicts two infrastructures employed on the experiments. In this second environment, instead of running the application to input data into the Blockchain locally, the script is hosted in a virtual machine (VM) on the Cloud. We configured an Amazon Web Services VM with the vital signs dataset. The input application runs in the VM and send requests to the Blockchain in our local infrastructure. This setup characterizes a Cloud environment because sensor data should use the Internet to reach the Blockchain. Given both local and Cloud infrastructures, we are able to compare them and show the results of employing FogChain.

At the end of the configuration stage, a Blockchain application was set in place with the Hyperledger Fabric Blockchain to store and manage PHR in a Fog environment. This preparation allowed us to collect metrics of this integration of technologies such as IoHT, Fog computing, and Blockchain, leading us to the next section where we finally execute all tests and assess the benchmark results.

D. EVALUATION SCENARIOS

One of the main goals of FogChain is to improve response time for IoHT applications. Therefore, we designed different evaluation scenarios to compare it with Cloud solutions in order to verify FogChain's applicability. Additionally, some parameter-wise decisions may influence the performance of the model. Thus, we also cover this analysis in the evaluation scenarios. The evaluation of FogChain was carried in three different phases. The first phase consists of discovering the optimal batch size of requests sent to the Blockchain that results in the best latency and TPS. The latency metrics and its calculation were carried by the execution of multiple end-to-end requests, thus calculating the average results in comparison with each other. It comprises ten executions of four different batch sizes: 50, 100, 200, and 1,000. This phase aims at evaluating weather the batch size impacts TPS or not.

In the second phase, three scenarios were modeled varying the batch size and the number of concurrent sessions. Table 3 presents the parameters employed in each scenario. For each scenario, the total number of requests is equal to 10,000 per session. The evaluation comprises the execution of each scenario ten times. Thus, TPS is achieve by averaging the results of the ten executions. For instance, let the total requests be 10,000, the average of ten executions be 100s, then $TPS = \frac{10{,}000}{100}$, resulting in 100 TPS.

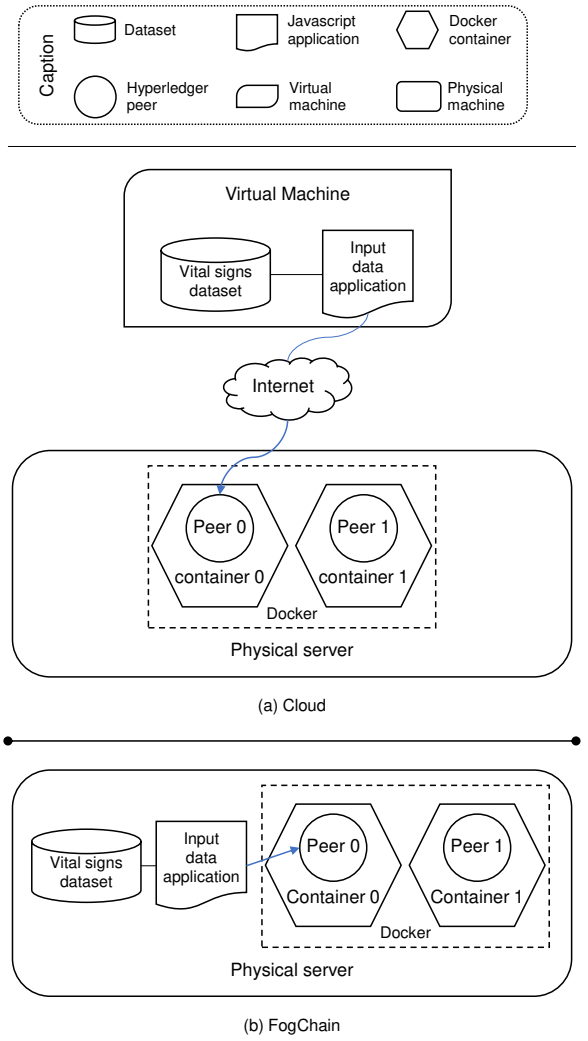

FIGURE 7. Cloud and FogChain infrastructures employed for experiments.

TABLE 3. Evaluation scenarios with different parameters.

Scenario	Batch Size	Concurrent Sessions
Light	50	10
Medium	50	50
Heavy	50	100

Finally, the third phase consists of comparing both FogChain to Cloud solutions. Therefore, we executed the same scenario in each infrastructure to compare the average latency in each one. More specifically, the scenario comprises 10 executions of the application sending a batch of 50 samples to the Blockchain in each infrastructure presented in Figure 7. Results are obtained by averaging the latency of the ten executions.

VI. RESULTS AND DISCUSSION

In this section we are going to demonstrate all results obtained during the research and development of our model implementation, carried simulations and benchmarks.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3109822, IEEE Access

A. BATCH SIZE EVALUATION

Determined to check how long it would take for a single transaction to completion under our Fog computing environment, we executed a initial test using the *add* operation from the Hyperledger Composer API, which expects only a single asset as input parameter. It resulted in an average $Latency$ of 180ms for a transaction to be created, ordered, validated and ultimately persisted in the ledger, which if executed multiple times sequentially would lead in approximately 5 TPS as throughput.

Seeking performance improvements, transactions were organized in bulks (batches) to verify a possible increase of throughput and for that, instead of sending transactions one by one sequentially, we employed the *addAll* operation, which expects as input parameter an array of assets, in our case, an array of vital signs readings. In other words, the interaction with our Blockchain network was changed to work in batches and the tricky part is to find an optimum batch size. This process implies our FogChain solution to accumulate data and organize them in an array structure before sending to the Blockchain. Figure 8 depicts the TPS achieved when employing different batch sizes, as described in Section V-D.

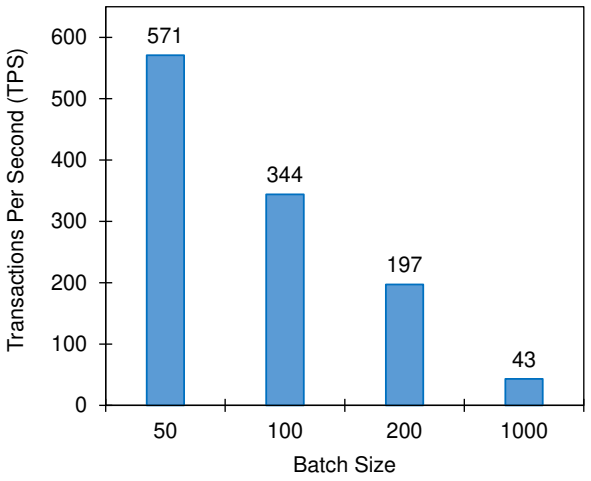

FIGURE 8. Multiple batch configuration benchmark results.

According to the figure, performance degradation was noticed while working with larger batch sizes. For example, a batch with 1,000 transactions would take approximately 23 seconds to completion, with an low average of 43 TPS, while a smaller batch with half transactions (500) would take only six seconds. It was the first indication that our optimum batch size was likely to be a smaller number.

B. ANALYSIS OF DIFFERENT SCENARIOS

Table 4 shows the obtained results for each evaluation scenario. The Light load achieved the best results for all metrics compared to the other two. In this particular scenario, the total number of requests is lower than the Medium and Heavy loads. Thus, it requires less CPU and Memory to compute all transactions. As a consequence, both TPS and $Latency$ achieved the best results. On the other hand, as the scenarios Medium and Load have more requests to compute, their final results increase according to it. For instance, the Medium load achieved higher results than the Light, and the Heavy achieved even higher.

For all scenarios, the batch size is equal, however, they achieve different TPS. The Light load obtained similar TPS to the tests performed to evaluate the batch size previously (see Figure 8). However, the same is not true for the Medium and Heavy scenarios. The results demonstrate that, even with the optimal batch size, the TPS is impacted according to the number of concurrent sessions. That imposes concurrency on processing requests, which decreases the final TPS.

C. FOGCHAIN VS CLOUD

The third phase of our experiments aims at evaluating the impact on $Latency$ when employing FogChain versus the employment of a Cloud environment. Figure 9 depicts the difference between the two infrastructures result from the experiments. FogChain ach2ieves a $Latency$ 62.6% smaller when compared to the Cloud environment. As the data and software components involved in running the experiments are the same, we conclude that the main reason for such a difference is the latency introduced by the Internet connection.

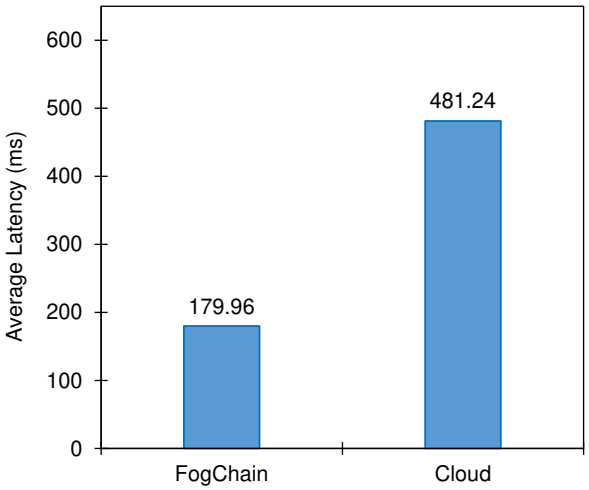

FIGURE 9. FogChain vs Cloud response-time comparison.

As depicted in Section 7, all software and data components are the same in both infrastructures. The only thing that changes from one setup to the other is the location where the input data is. When employing a Cloud environment, the data should be forwarded to the system through the internet connection, which may route data traffic in different paths depending on the Internet providers. On the other hand, when employing FogChain, the Blockchain infrastructure is closer to the data source. That avoids delays imposed by routing

TABLE 4. Average results from ten executions each at Fog environment with 95% confidence interval.

Rated item	Light Load	Medium Load	Heavy Load
CPU usage (%)	9%	15.4%	18.53%
Memory usage (%)	27%	43.3%	59.5%
Throughput (TPS)	579 ± 2.33 (σ = 3.76)	502 ± 3.3 (σ = 5.32)	453 ± 4.41 (σ = 7.12)
Latency (ms)	169 ± 1.2 (σ = 1.93)	185 ± 1.73 (σ = 2.79)	193 ± 2.81 (σ = 4.53)

protocols from public internet providers, thus, improving the results.

D. DISCUSSION

FogChain focuses on employing Fog Computing to bring Blockchain closer to PHR IoT devices. The main goal is to decrease response time on registering records in the Blockchain, making them available quicker. This strategy makes the solution independent from Cloud infrastructures. At the same time, as it employs several Fog nodes, the infrastructure can be easily scaled by adding more nodes with Blockchain peers. Despite that, the evaluation we employ focuses on proving the performance improvement in response time for application. The implemented evaluation demonstrated the capacity of our architecture as a technology integrator, providing an alternative to traditional Cloud-IoT solutions, and the obtained results for latency and throughput metrics did highlight the performance boost driven by the Fog computing adoption.

Having complete patient's medical history available in loco turns to be an intangible benefit for the healthcare domain, leaving the solution with no external dependencies such as ISP and or services, which is in contrast, for example, with previous models assessed in the related work section.

The FogChain implementation for PHR management demonstrated a slice of how Blockchain could be employed in the healthcare domain, benefiting from its cryptographic and tamper-proof nature, which adds an additional security layer so necessary for healthcare applications. However, the FogChain model is not limited to the healthcare domain only and could be also adapted to other domains, for example supply chain, smart-city, and cross-industry applications.

Moreover, working with batches of transactions demonstrated to be favorable, and with this approach in place, we managed to obtain a satisfactory application throughput. It resulted in performance improvements on TPS capacity of our architecture and combined with the local Fog computing benefits, promoted closer to real-time features on the process of vital signs' collecting, securing and storage. As bandwidth measures how much data can flow through a specific connection at one time, it turns out it strongly relies on the physical hardware used in the experiment. For instance, a gigabit Ethernet connection has a bandwidth of 1,000 Mbps, while the Fast Ethernet compliant network may transfers data at rates up to 100 Mbps. Thus, considering the local nature of the Fog, its bandwidth relies on the local infrastructure itself while the Internet Service Providers (ISP) restrain it in cloud-like environments. More specifically, in our scenario, the patient's wearable sensors usually collect and transfer raw data, which are typically lightweight, not consuming extensive network bandwidth. However, the more the sensors evolve, the more they need larger bandwidth on the network.

VII. CONCLUSION

It is safe to say that Fog computing can play a big role in healthcare applications, providing local processing power, services, and increasing resources availability. It allows applications to decrease the amount of access to the cloud, where the connection is subject to delays on worldwide network traffic, turning to be a viable and potential integrator of IoHT and Blockchain technologies. The current state-of-the-art focuses on providing Blockchain solutions for healthcare with Cloud computing support. Therefore, it inherits the latency of network connections to reach Cloud infrastructures. In this context, FogChain aims at bringing the Blockchain infrastructure closer to the healthcare environment decreasing latency for its operations. Its main contribution relies on a Fog infrastructure encompassing Blockchain peers for validation of PHR operations.

The implementation's evaluation demonstrated satisfactory proofs regarding the feasibility of FogChain architecture and the combination of its components. A possible future direction to this research could be carrying tests it in clinics and hospitals scenario. Some challenges were identified during our research and development process, such as technological limitations, industry adoption, infrastructure costs, among others. Furthermore, currently available frameworks may not have full compliance with the healthcare regulatory organizations such as HIPAA and GDPR. For example, in a scenario where a patient has the right to be forgotten, requiring the entire deletion of their stored health data in the network, which would clash directly with the immutability principle of Blockchain solutions.

The need for more investment and efforts to consolidate open standards for health records data structure has become clear and yet challenging, improving its levels of interoperability among health providers could end-up easing the Blockchain adoption from the healthcare industry players. Furthermore, our model itself does not solve the intrinsic interoperability issues regarding different data formats between health providers, which are a broader concern in the healthcare area. Another important variable that must be taken into account when considering the Blockchain solution is the scalability constraints in terms of the trade-off between the volume of transaction and computer power for processing time of transactions.

Finally, our solution has some limitations that can be addressed in future work. First, the Fog infrastructure we employ is based on a single server running containers. The ideal setup can consider employing less powerful nodes distributed physically instead of virtualized ones in the same physical machine. In addition, the evaluation does not consider scenarios with different nodes available, which would be required to assess the scalability of the solution. Second, we developed a single application to extract data from a dataset and input it into the system. Further research should be done employing real-time critical applications instead. Third, the evaluation focuses mainly few parameters and metrics, which future experiments can explore further. Finally, another point of attention is on the evaluation scenarios. We do suggest adding more participants and roles to the network, for example, allowing insurance companies to join the network, moreover, proposing and implementing interoperability features for the PHR storage, regarding data format and transaction block structures.

DECLARATION OF COMPETING INTEREST

The authors declare that there is "No Conflict of Interest" in the current manuscript.

ACKNOWLEDGMENTS

The authors would like to thank the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - CAPES (Finance Code 001), a foundation for higher education personnel improvement linked to the Brazilian Ministry of Education and Conselho Nacional de Desenvolvimento Científico e Tecnológico - CNPq (Grant Number 309537 / 2020-7), which is a National Council of Brazilian Ministry of Science, Technology, Innovations and Communications created for Scientific and Technological Development and encourage research in Brazil for supporting this work.

REFERENCES

[1] Eshtiak Ahmed, Ashraful Islam, Mohsena Ashraf, Atiqul Islam Chowdhury, and Mohammad Masudur Rahman. Internet of Things (IoT): Vulnerabilities, Security Concerns and Things to Consider. In 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), pages 1–6. IEEE, 2020.

[2] Raifa Akkaoui, Xiaojun Hei, and Wenqing Cheng. EdgeMediChain: a hybrid edge blockchain-based framework for health data exchange. Ieee Access, 8:113467–113486, 2020.

[3] Sadia Ali, Yaser Hafeez, N. Z. Jhanjhi, Mamoona Humayun, Muhammad Imran, Anand Nayyar, Saurabh Singh, and In-Ho Ra. Towards pattern-based change verification framework for cloud-enabled healthcare component-based. Ieee Access, 8:148007–148020, 2020.

[4] Shaimaa Badr, Ibrahim Gomaa, and Emad Abd-Elrahman. Multi-tier blockchain framework for iot-ehrs systems. Procedia Computer Science, 141:159–166, 2018.

[5] Kamanashis Biswas and Vallipuram Muthukkumarasamy. Securing smart cities using blockchain technology. In 2016 IEEE 18th international conference on high performance computing and communications; IEEE 14th international conference on smart city; IEEE 2nd international conference on data science and systems HPCC/SmartCity/DSS, pages 1392–1393. IEEE, 2016.

[6] Rajkumar Buyya and Jungmin Son. Software-defined multi-cloud computing: A vision, architectural elements, and future directions. In International Conference on Computational Science and Its Applications, pages 3–18. Springer, 2018.

[7] Victor R Basili1 Gianluigi Caldiera and H Dieter Rombach. The goal question metric approach. Encyclopedia of software engineering, pages 528–532, 1994.

[8] Edward C Cheng, Ying Le, Jia Zhou, and Yang Lu. Healthcare services across china–on implementing an extensible universally unique patient identifier system. International Journal of Healthcare Management, 113: 210–216, 2018.

[9] Konstantinos Christidis and Michael Devetsikiotis. Blockchains and smart contracts for the internet of things. Ieee Access, 4:2292–2303, 2016.

[10] Marco Conoscenti, Antonio Vetro, and Juan Carlos De Martin. Blockchain for the internet of things: A systematic literature review. In 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications AICCSA, pages 1–6. IEEE, 2016.

[11] Marek A Cyran. Blockchain as a foundation for sharing healthcare data. Blockchain in Healthcare Today, 2018.

[12] Cristiano André da Costa, Cristian F Pasluosta, Björn Eskofier, Denise Bandeira da Silva, and Rodrigo da Rosa Righi. Internet of health things: Toward intelligent vital signs monitoring in hospital wards. Artificial Intelligence In Medicine, 2018.

[13] Gaby G Dagher, Jordan Mohler, Matea Milojkovic, and Praneeth Babu Marella. Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. Sustainable cities and society, 39:283–297, 2018.

[14] Carlo Demichelis and Philip Chimento. Ip packet delay variation metric for ip performance metrics ippm. The Internet Society, 2002.

[15] Ali Dorri, Salil S Kanhere, Raja Jurdak, and Praveen Gauravaram. Blockchain for iot security and privacy: The case study of a smart home. In 2017 IEEE International Conference on Pervasive Computing and Communications Workshops PerCom Workshops, pages 618–623. IEEE, 2017.

[16] Ariel Ekblaw, Asaph Azaria, John D Halamka, and Andrew Lippman. A case study for blockchain in healthcare:"medrec" prototype for electronic health records and medical research data. In Proceedings of IEEE open & big data conference, volume 13, page 13, 2016.

[17] Lars Hagge and Jens Kreutzkamp. A benchmarking method for information systems. In Proceedings. 11th IEEE International Requirements Engineering Conference, 2003., pages 245–253. IEEE, 2003.

[18] Muneeb Ul Hassan, Mubashir Husain Rehmani, and Jinjun Chen. Privacy preservation in blockchain based iot systems: Integration issues, prospects, challenges, and future research directions. Future Generation Computer Systems, 97:512–529, 2019.

[19] Tripathi, Gautami and Ahad, Mohd Abdul and Paiva, Sara. S2HS-A blockchain based approach for smart healthcare system. Healthcare, pages 100391. Elsevier, 2019.

[20] Daisuke Ichikawa, Makiko Kashiyama, and Taro Ueno. Tamper-resistant mobile health using blockchain technology. JMIR mHealth and uHealth, 57:e111, 2017.

[21] Jayneel Vora, Anand Nayyar, Sudeep Tanwar, Sudhanshu Tyagi, Neeraj Kumar, M. S. Obaidat, and Joel J P C Rodrigues. BHEEM: A blockchain-based framework for securing electronic health records. In 2018 IEEE Globecom Workshops (GC Wkshps), pages 1–6. IEEE, 2018.

[22] Elena Karafiloski and Anastas Mishev. Blockchain solutions for big data challenges: A literature review. In IEEE EUROCON 2017-17th International Conference on Smart Technologies, pages 763–768. IEEE, 2017.

[23] Avinash Kaur, Anand Nayyar, and Parminder Singh. BLOCKCHAIN. Cryptocurrencies and Blockchain Technology Applications, pages 25–42 John Wiley & Sons, Ltd, 2020.

[24] Minhaj Ahmad Khan and Khaled Salah. Iot security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems, 82: 395–411, 2018.

[25] Barbara Kitchenham, Rialette Pretorius, David Budgen, O Pearl Brereton, Mark Turner, Mahmood Niazi, and Stephen Linkman. Systematic literature reviews in software engineering–a tertiary study. Information and software technology, 528:792–805, 2010.

[26] Tsung-Ting Kuo, Hyeon-Eui Kim, and Lucila Ohno-Machado. Blockchain distributed ledger technologies for biomedical and health care applications. Journal of the American Medical Informatics Association, 246: 1211–1220, 2017.

[27] Rana M. Amir Latif, Khalid Hussain, N. Z. Jhanjhi, Anand Nayyar, and Osama Rizwan. A remix IDE: smart contract-based framework for the healthcare sector by using Blockchain technology. Multimedia Tools and Applications, pages 1–24, 2020.

[28] Victoria L Lemieux. A typology of blockchain recordkeeping solutions and some reflections on their implications for the future of archival preservation. In 2017 IEEE International Conference on Big Data Big Data, pages 2271–2278. IEEE, 2017.

[29] David Liu, Matthias Görges, and Simon A. Jenkins. University of queensland vital signs dataset. Anesthesia & Analgesia, 1143:584–589, mar 2012. . URL https://doi.org/10.1213/ane.0b013e318241f7c0.

[30] Katiuscia Mannaro, Gavina Baralla, Andrea Pinna, and Simona Ibba. A blockchain approach applied to a teledermatology platform in the sardinian region italy. Information, 92:44, 2018.

[31] André Henrique Mayer, Cristiano André da Costa, and Rodrigo da Rosa Righi. Electronic health records in a blockchain: A systematic review. Health Informatics Journal, page 1460458219866350, 2019.

[32] GHASSEM Mokhtari, AMJAD Anvari-Moghaddam, and QING Zhang. A new layered architecture for future big data-driven smart homes. IEEE Access, 2019.

[33] Sue B Moon, Paul Skelly, and Don Towsley. Estimation and removal of clock skew from network delay measurements. In IEEE INFOCOM'99. Conference on Computer Communications. Proceedings. Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies. The Future is Now Cat. No. 99CH36320, volume 1, pages 227–234. IEEE, 1999.

[34] M Niranjanamurthy, BN Nithya, and S Jagannatha. Analysis of blockchain technology: pros, cons and swot. Cluster Computing, pages 1–15, 2018.

[35] Oscar Novo. Blockchain meets iot: An architecture for scalable access management in iot. IEEE Internet of Things Journal, 52:1184–1195, 2018.

[36] Jianli Pan and James McElhannon. Future edge cloud and edge computing for internet of things applications. IEEE Internet of Things Journal, 51: 439–449, 2018.

[37] Kefa Rabah. Challenges & opportunities for blockchain powered healthcare systems: A review. Mara Research Journal of Medicine & Health Sciences-ISSN 2523-5680, 11:45–52, 2017.

[38] Md Abdur Rahman, Md Mamunur Rashid, M Shamim Hossain, Elham Hassanain, Mohammed F Alhamid, and Mohsen Guizani. Blockchain and iot-based cognitive edge framework for sharing economy services in a smart city. IEEE Access, 7:18611–18621, 2019.

[39] Ana Reyna, Cristian Martín, Jaime Chen, Enrique Soler, and Manuel Díaz. On blockchain and its integration with iot. challenges and opportunities. Future generation computer systems, 88:173–190, 2018.

[40] Ron Ribitzky, James St Clair, David I Houlding, Chrissa T McFarlane, Brian Ahier, Michael Gould, Heather L Flannery, Erik Pupo, and Kevin A Clauson. Pragmatic, interdisciplinary perspectives on blockchain and distributed ledger technology: paving the future for healthcare. Blockchain in Healthcare Today, 2018.

[41] Alex Roehrs, Cristiano André da Costa, and Rodrigo da Rosa Righi. Omniphr: A distributed architecture model to integrate personal health records. Journal of biomedical informatics, 71:70–81, 2017a.

[42] Alex Roehrs, Cristiano André Da Costa, Rodrigo da Rosa Righi, and Kleinner Silva Farias De Oliveira. Personal health records: a systematic literature review. Journal of medical Internet research, 191:e13, 2017b.

[43] Alex Roehrs, Cristiano André da Costa, Rodrigo da Rosa Righi, Valter Ferreira da Silva, José Roberto Goldim, and Douglas C Schmidt. Analyzing the performance of a blockchain-based personal health record implementation. Journal of biomedical informatics, page 103140, 2019.

[44] Mayra Samaniego and Ralph Deters. Blockchain as a service for iot. In 2016 IEEE International Conference on Internet of Things iThings and IEEE Green Computing and Communications GreenCom and IEEE Cyber, Physical and Social Computing CPSCom and IEEE Smart Data SmartData, pages 433–436. IEEE, 2016.

[45] Zonyin Shae and Jeffrey JP Tsai. On the design of a blockchain platform for clinical trial and precision medicine. In 2017 IEEE 37th International Conference on Distributed Computing Systems ICDCS, pages 1972–1980. IEEE, 2017.

[46] Pradip Kumar Sharma, Mu-Yen Chen, and Jong Hyuk Park. A software defined fog node based distributed blockchain cloud architecture for iot. IEEE Access, 6:115–124, 2018.

[47] Bingqing Shen, Jingzhi Guo, and Yilong Yang. Medchain: Efficient healthcare data sharing via blockchain. Applied Sciences, 96:1207, 2019.

[48] Cícero A Silva, Gibeon S Aquino, Sávio RM Melo, and Dannylo JB Egídio. A fog computing-based architecture for medical records management. Wireless Communications and Mobile Computing, 2019, 2019.

[49] Simar Preet Singh, Anand Nayyar, Rajesh Kumar, and Anju Sharma. Fog computing: from architecture to edge computing and big data processing. The Journal of Supercomputing volume, 75:2070-2105, 2019.

[50] Fuad Suad, Cristiano André Da Costa, Rodrigo da Rosa Righi, Márcio Gomes, and Luiz Bertoldi. Exploring extensibility and interoperability in the internet of things landscape. In Pedro Isaías and Hans Weghorn, editors, 17th International Conference on WWW/Internet 2018, pages 339–343, 2018, Budapeste. PROCEEDINGS OF THE INTERNATIONAL CONFERENCES ON WWW/INTERNET 2018 AND APPLIED COMPUTING 2018. Lisboa, 2018. IADIS.

[51] Caixiang Fan, Sara Ghaemi, Hamzeh Khazaei, and Petr Musilek Performance Evaluation of Blockchain Systems: A Systematic Survey. Ieee Access, 8:126927–126950, 2020.

[52] Shreshth Tuli, Redowan Mahmud, Shikhar Tuli, and Rajkumar Buyya. Fogbus: A blockchain-based lightweight framework for edge and fog computing. Journal of Systems and Software, 2019.

ANDRÉ HENRIQUE MAYER is a research assistant at Universidade do Vale do Rio dos Sinos (UNISINOS), Brazil. Currently, he holds a Master's degree in Applied Computing Graduate Program at UNISINOS, and he is PhD candidate at the same university, since 2020. His research interests include Blockchain and Internet-of-Things.

VINICIUS FACCO RODRIGUES received the Ph.D. degree in Applied Computing from the University of Vale do Rio dos Sinos (UNISINOS), Brazil, in 2020. He is a research assistant from the Software Innovation Laboratory – SOFTWARELAB at UNISINOS since 2016 working on research projects. His research interests include: distributed systems, computer networks, high-performance computing, health informatics, and artificial intelligence.

CRISTIANO ANDRÉ DA COSTA is a full professor at Universidade do Vale do Rio dos Sinos (Unisinos), Brazil, and a researcher on productivity at CNPq (National Council for Scientific and Technological Development). His research interests include ubiquitous, mobile, parallel and distributed computing. He is a senior member of the ACM and IEEE. He is also a member of IADIS and the Brazilian Computer Society (SBC).

RODOLFO ANTUNES is an assistant professor and researcher at UNISINOS. He holds a B.Sc. degree in Computer Science from UNISINOS (2009) and a Ph.D. degree in Computer Science from UFRGS (2016). His research interests include Internet-of-Things and Distributed Systems.

RODRIGO RIGHI is assistant professor and researcher at University of Vale do Rio dos Sinos, Brazil. Rodrigo concluded his post-doctoral studies at KAIST — Korea Advanced Institute of Science and Technology, under the following topics: RFID and cloud computing. He obtained his Ph.D. degree in Computer Science from the UFRGS University, Brazil, in 2009. His research interests include load balancing and process migration. He is a member of the IEEE and ACM.

ALEX ROEHRS is an assistant professor and researcher at Universidade do Vale do Rio dos Sinos (UNISINOS). He holds a Ph.D. degree in Computer Science from the Universidade do Vale do Rio dos Sinos (UNISINOS, 2019). His research interests include Distributed Systems, Blockchain and Health Informatics.